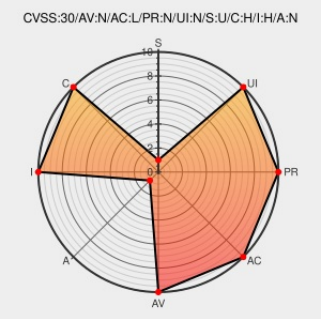
CVE-2017-8805

Published on: 10/17/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:43 PM UTC

CVE-2017-8805

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ftpsync from Debian contain the following vulnerability:

Debian ftpsync before 20171017 does not use the rsync --safe-links option, which allows remote attackers to conduct directory traversal attacks via a crafted upstream mirror.

CVE-2017-8805 has been assigned by security@debian.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Ask rsync to only allow save symlinks (d1ca2ab2) · Commits · Debian Mirror team / archvsync · GitLab	Issue Tracking, Patch, Vendor Advisory, anonscm.debian.org, text/html	CONFIRM anonscm.debian.org/cgit/mirror/archvsync.git/commit/?id=d1ca2ab2210990b6dfb664cd6776a41b71c48016

oss-security - CVE-2017-8805: Unsafe symlinks not filtered in Debian mirror script ftpsync	Issue Tracking Mailing List Patch Third Party Advisory www.openwall.com text/html	CONFIRM www.openwall.com/lists/oss-security/2017/10/17/2
New ftpsync version 20171017 (security update)	Issue Tracking Mailing List Vendor Advisory lists.debian.org text/html	CONFIRM lists.debian.org/debian-mirrors/2017/10/msg00017.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Debian	Ftpsync	All	All	All	All

cpe:2.3:a:debian:ftpsync:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→